GENERAL GOVERNMENT

Opinion polls show that public trust in government has hit record lows in recent years, leading some to conclude that government claims of Y2K-compliance progress cannot be believed. The Committee refutes that conclusion in light of abundant evidence that federal agencies and state and local governments are indeed fixing the Y2K problems in their own systems.

Not all government agencies are 100% ready, and not everyone has taken the problem equally seriously. However, enough effort, time, and money has been spent for the Committee to conclude that, overall, federal agencies will continue to function, state governments will continue to govern, and local bodies will continue to deliver services in most localities.

FEDERAL AGENCIES

Background and Vulnerabilities

If the effort to reach Y2K readiness is a race, most of the federal government is crossing the finish line. For those still lagging, the hurdles lie in completing work on remaining mission-critical systems and conducting end-to-end testing, both internally and with external partners. Many agencies must finish developing realistic contingency plans and communicate them to the public. The size and complexity of the problems with Department of Defense systems warrants a separate discussion, which follows this section of the report.

An extremely wide variety of information technology systems, in age and type, are in use throughout the federal government. These systems, which have myriad Y2K problems, control and manage large data sets on every conceivable subject, and are crucial to the payment of benefits, the management of loans, the issuance of currency, defense, taxation, the guarantee of public safety and welfare; in short, nearly every federal program. The silver lining in the Y2K stormcloud has been the opportunity to eliminate unnecessary legacy systems and to revise and improve existing systems.

During the past three years of intensive Y2K work, agencies that had already achieved some measure of Y2K compliance, like the Social Security Agency and the Department of Defense, led the charge and shared important lessons such as involving senior management in Y2K remediation programs. However, the late start by many agencies necessitated a shift in focus to mission-critical systems. These are the systems an agency requires to adequately fulfill its function. There are more than 6,000 mission-critical systems at the 24 major federal agencies.

This process of mission-critical triage for Y2K has meant that non-mission critical systems, which may have important implications for public confi-

dence, and interconnections with mission-critical systems have not been fully remediated or rigorously tested. Moreover, the problem of non-Y2K compliant systems is complicated by the interconnectedness of agencies at the federal, state, tribal, and local levels. The ability to adequately and fully test multiple systems end-to-end lies somewhere between unlikely and improbable. Further, federal agencies have a history of failing to complete IT-related projects on time and within budget. As a result, agencies have rightly dealt with these residual vulnerabilities by developing contingency plans for systems, processes, and organizational functions. If they have not, they remain at risk.

What Is Being Done?

Federal agencies' progress is tracked through quarterly reporting to the Office of Management and Budget (OMB), which then issues a summary report. There have been ten reports since the first one in February 1997, and the latest was released on September 13, 1999.

As insurance against unknown problems, these agencies have been developing business continuity and contingency plans (BCCPs) at OMB's request. BCCPs are contingency plans that include a plan to restart or continue business functions regardless of operational conditions. OMB imposed a June 15, 1999, deadline for agencies to submit their BCCPs, and OMB is currently evaluating and providing feedback on these plans. OMB has instructed agencies to demonstrate Year 2000 operational plans, including BCCPs, by September 30, 1999.

In the June quarterly report, OMB began tracking 43 high-impact federal programs and individual state preparedness for 10 federally sponsored, state-run programs, such as Medicaid, Women with Infants and Children (WIC), and unemployment insurance. GAO has published Y2K guides and continues to audit high-risk areas, including these high-impact federal programs.

The President's Y2K Council was formed in February 1998. Twenty-five industry sector working groups consisting of public and private partnerships have been established. These working groups have been instrumental in promoting Y2K awareness to wider audiences and preparing industry sector Y2K status assessments. The Council has also introduced a new toll-free telephone number (888-USA-4-Y2K) to provide Y2K information to consumers.

Both the Senate and House continue to hold public hearings on a variety of Y2K related topics. While the House has focused more on federal agencies and programs, the Committee has focused on the private sector and on the interaction of federal agencies with other sectors. The Committee held a hearing on April 14, 1999 to follow-up on the March 31 deadline for completing mission-critical remediation.[1] The Committee also held a joint hearing with the Appropriations Committee on federal government Y2K expenditures in June 1999. [2]

The President's Y2K Council is in the process of building an Information Coordination Center (ICC) to collect information, monitor the situation, and solve problems over the transition period (November 1999-January 2000). More information about the ICC is found in a separate subsection of this report.

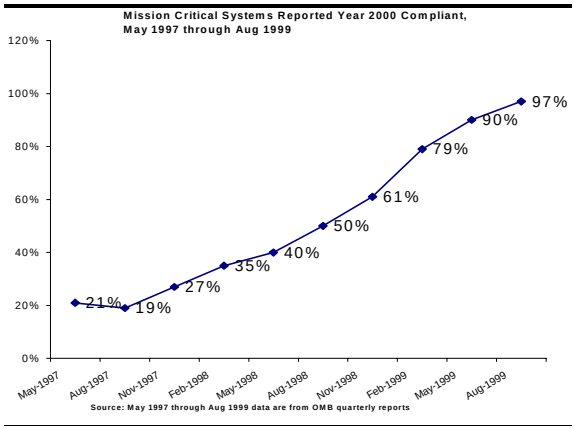
Status

All mission-critical systems for the federal government were to have been remediated and tested by March 1999. Although the President's Y2K Council reported that the federal government was 93% ready by March 1999, later testimony by the Director of OMB indicated that this milestone wasn't reached until early June,[3] giving at least the impression that the government was stalled on Y2K activities for three months.

The rest, some 500 mission-critical systems, were expected to reach Y2K readiness well before December 31, 1999. OMB's September 15 quarterly report indicates that federal agencies have certified 97% of their systems as Y2K compliant, truly an impressive jump from the 35% ready in February 1998. Importantly, the government's testing regime is following standards established by the National Institute for Standards and Technology (NIST).[4] This may account for the lag in independently certifying systems Y2K ready.

Federal agencies are appropriately shifting focus and emphasis to business continuity and contingency planning development and testing, but the cost of implementing such plans has not yet been determined. In addition, major differences exist in methodology between federal agencies, despite the fact that OMB provided specific guidance.[5]

Problems with the plans include lack of consistency between different divisions of an agency, inappropriate focus on computer systems instead of business processes, and vague plans for coordinating emergency operation plans. The scope of the plans varies, with approximately



10,000 different plans for individual departments of the major agencies. OMB guidance for the development of BCCPs includes the directive to identify risk factors for each core business function and associated system, assign them a probability rating for risks, and then an impact rating.

As an illustration, the FAA lists the risks associated with the failure of a particular tracking system, assigns the probability of failure (low), and then describes backup processes or systems. One entry in the risk matrix is as follows:

Business process	Air Traffic System, (SURVEILL.1)
Environment	Terminal
Risk	Degradation of ASDE or AMASS may adversely impact the controllers ability to efficiently identify and safely separate aircraft on the ground especially during inclement weather or non-daylight hours.
Probability	1 (1 is lowest, 10 is highest)
Impact	10 (10 would immediately stop operations)
Business Priority	30 (Probability X Impact X Weight for overall importance of process)
Risk Mitigation Strategy	ASDE is Y2K compliant and AMASS has completed renovation.
Contingency plan	Invoke the local facility level contingency plan prescribed by FAA Orders 1900.47 and 6030.31. Revert to visual observation procedures. Notify A0A-4 that the contingency plan is in effect and when normal operations are resumed.

The Committee also asked agencies for information regarding their responsibilities under the Federal Response Plan, which is used in emergency situations. Although agencies could identify their statutory obligations under the plan, the relationship with Y2K-generated contingencies were vague or absent. The Department of Defense, covered in more detail later, has given its civilian responsibilities a low priority. On the other hand, FEMA, which would implement the plan, remains a strong force in providing leadership.

Overall, the Committee finds that the data is available to evaluate the progress of the federal government; that it has been disclosed to the public; and that independent validation and verification (IV&V) of remediated systems has been occurring. One area of remaining concern is the pace of data exchange testing. In OMB's latest quarterly report, the agencies reported on completion date for testing data exchanges with other federal agencies, states, foreign governments, and private sector entities.

Work will be completed in:	*For the following agencies:*
December	Dept of Justice, Federal Emergency Management Agency, Dept of the Treasury
November	Dept of Transportation, Environmental Protection Agency
October	NASA, National Science Foundation
September	Dept of Agriculture, Dept of State, Social Security Admin, Office of Personnel Management, Small Business Administration
August	Veterans Affairs, Dept of Energy
DONE	Commerce, Education, Health & Human Services, Housing & Urban Development, Interior, Labor, Agency for International Development, General Services Administration, Nuclear Regulatory Agency

In the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, (Public Law No. 105-277), Congress provided $3.35 billion in emergency supplemental funding--$1.1 billion for the Department of Defense and $2.25 billion for non-Defense agencies. Funds are to remain available until September 30, 2001. There have been nine allocations against this emergency supplemental.[6] There are no funds remaining for Defense and (as of August 1999) $292.3 million remains for non-Defense. Although these funds were specifically designed to last until well after January 1, 2000, little remains for implementing contingency plans, further end-to-end testing, and cleaning-up problems next year.

In addition to the emergency funds, agencies have used programmatic and general information system

funds for Y2K programs and the cost of replacing equipment and software. The current cost estimate for the 24 major agencies exceeds $8 billion, more than triple the agencies' original estimate of $2.3 billion from OMB's first quarterly report in February 1997. Notably poor in correctly estimating Y2K costs were HHS and the Departments of Interior, Justice, Transportation, and Treasury, as summarized in the table below. The enormous growth in Y2K budgets can be partly attributed to the key role these agencies play in administering state-run programs.

Funding Estimates for Y2K Remediation

Agency	Feb-97	May-99	% Increase
HHS	$ 90.70	$ 816.80	801%
Interior	$ 11.30	$ 115.70	924%
Justice	$ 22.10	$ 163.60	640%
Transportation	$ 80.40	$ 345.80	330%
Treasury	$ 318.50	$ 1,566.20	392%

The result of spending $8 billion on Y2K instead of other IT projects will be a pent-up demand for system modifications or modernization. Indeed, agencies have, at times, asked that lawmakers not require them to implement new rules in 1999 to avoid making Y2K remediation more difficult. According to testimony of the Comptroller General of the U.S., *"…demands – including system enhancements and computer security – have not vanished; in fact, they have grown*."[7]

OMB stopped assessing the agencies according to a three-tiered approach but, as of March 18, 1999, the U.S. Agency for International Development (USAID), HHS, and the Department of Transportation (DOT) were demonstrating insufficient evidence of progress. These three agencies were invited to testify before the Committee on April 14, 1999.[8]

Criticism of the efforts of HHS, in particular, the Health Care Financing Administration (HCFA), have resulted in a vastly improved picture, as detailed in this report's section on healthcare. According to the Deputy Secretary of HHS:

"*We have required our operating divisions or agencies to report monthly on their systems renovation, the progress in making their data exchanges compliant, their status on making their personal computers, telecommunications, hardware and software, facilities and biomedical equipment compliant. We require the agencies to have mission critical systems independently verified and validated. We are beginning the end-to-end testing phase to ensure that all of our independent systems function properly together.*" [9]

The potential for bad actors to attempt to defraud the government during a Y2K failure remains a concern. The Deputy Secretary of HHS testified, "…*HCFA's contingency plans provide mechanisms to ensure that providers' claims will get processed and paid even if parts of HCFA's system experience unanticipated failure. In addition, we will have in place at the turn of the millenium as we do today, financial and audit controls to help protect the integrity of the Medicare Trust Funds.*"[10] In briefings to Committee staff, HCFA provided specifics on an

impressive array of tactics to prevent fraud[11].

USAID has said that late readiness dates for its seven mission-critical systems reflected the need to ensure that systems were fully remediated and tested at international posts. "*The agency set a standard that repairs for compliance would be proven to work through testing not only in the computer lab, but also in the field where the USAID program is managed*."[12] As Senator Dodd noted, fixing seven systems is a lot easier than fixing the thousands of systems at the Department of Defense.

There is concern that agencies that have failed to fully test in the field cannot confidently claim Y2K readiness. For instance, according to a GAO report released in August 1999, the Small Business Administration (SBA) needs to strengthen systems testing. The report notes that "*weaknesses in SBA's Y2K testing increase the risk that its mission-critical are not yet Y2K ready*." If not adequately addressed, the Y2K computing problem poses significant risks to SBA's ability to provide financial, technical, and management assistance to more than 490,000 small businesses nationally, as well as disaster recovery assistance to individuals, families, and business services. SBA has responded that testing occurred with typical daily, weekly, and monthly data, and officials stated they will implement GAO recommendations to ensure adequate testing.

Non-mission critical systems could be the Achilles heel for agencies. The Social Security Administration experienced a glitch in a letter writing program on September 7, sending out 32,000 letters saying that as of January 1, **1900**, benefits would change for recipients of the letters. Although the mission-critical systems that generated the list of beneficiaries was fixed, a small problem in the letter printing application has created a public relations headache.

As highlighted in the subsequent section on state and local governments, several states are lagging behind in getting their systems Y2K ready to administer federal programs. Of the 43 high-impact federal programs now tracked by OMB, only two were Y2K ready as of the June 1999 OMB report. By August 14, the number of programs that had been fully and independently verified Y2K-ready had jumped to seven, and eight more expected to complete end-to-end testing by the end of August.

Of the remaining programs, all of which affect millions of Americans, eight more expect independent verification by the end of September, and 10 report completion dates at the end of October. The final 10 programs are the federally-supported, state-run programs, which expect to finish in November and December. The 28 programs not deemed Y2K ready as of this report include Child Nutrition Programs, Women with Infants and Children, Indian Health Services, Temporary Assistance for Needy Families, Child Support Enforce-

ment, Low Income Home Energy Assistance Program, Public Housing, and State Employment Security Agencies.

Expectations

By and large, federal agencies will complete work on their systems before December 31. It is likely, however, that no matter how prepared agencies are, there will be some unexpected Y2K problems in their systems or their systems' interfaces.

With less than $300 million dollars in emergency supplemental funding remaining, and much work that is continuing in the areas of BCCPs, testing, and IV&V, additional emergency funds will be needed. Further, if BCCPs must be implemented due to anticipated Y2K problems, the costs of implementation will cause costs to rise even further.

A number of states will not complete remediation and testing of systems used to support the administration of federal programs that are state-run. It is likely that agency BCCPs will need to be executed to ensure that eligible beneficiaries of those programs still receive benefits and the programs are properly administering benefits and accounting for them.

Expected failures may include one or more of the following and can be characterized as disruptive and inconvenient:

- disruptions in air travel schedules and congestion at airports;
- isolated problems with state-implemented programs such as child support tracking; and
- information collection problems with respect to various regulatory agencies.

Managing public reaction and supporting a coordinated response to large problems will be the ICC's mission. The Committee believes the formation of the ICC, as well as the related International Y2K Information Center, must progress much faster. The proper thresholds for reporting Y2K-related glitches and the processes for interacting with other key agencies and the private sector must be determined and communicated. These information flows will be critical, especially as it relates to the decision-making process in the White House. Moreover, the allocation of scarce resources for repairing systems or running contingency plans will need to be explained in greater detail to ensure the best use of funds and manpower.

DEPARTMENT OF DEFENSE

Background and Vulnerabilities

The Department of Defense (DOD), the largest federal agency with nearly half of the federal government's computer assets, continued to make significant progress tackling the Herculean management challenge posed by Y2K. The department relies on computer systems to conduct nearly all of its functions,

including strategic and tactical military operations; sophisticated weaponry; intelligence collection, analysis, and dissemination; security efforts; and more routine business operations such as payroll and logistics.

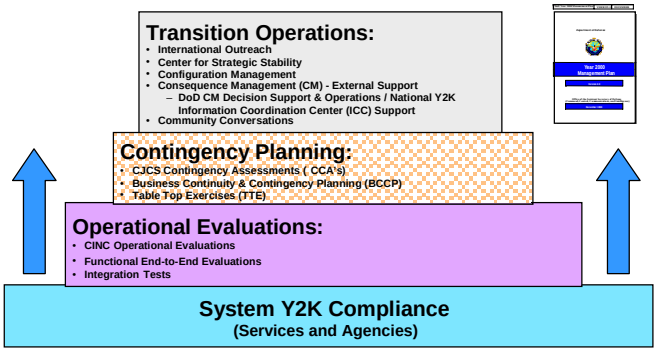
The problem confronting DOD is enormous in both breadth and complexity: it has more than 1.5 million computers, 28,000 automated information systems and 10,000 networks. Its information systems are linked by thousands of interfaces that exchange data within DOD and across organizational and international lines. Further, DOD's reliance on computer systems is increasing as technology changes the traditional concepts of warfighting through improved intelligence and rapidly modernized command and control. Successful defense operations will depend greatly on the department's ability to ensure that its systems and the systems with which they interface are Y2K compliant.

What is Being Done?

It is widely known that to effectively manage a successful enterprise-wide Y2K program, personal executive level emphasis and involvement is paramount. Dr. John J. Hamre, Deputy Secretary of Defense, has led the DOD attack against the Y2K bug from the front and his efforts have been instrumental in the strong performance that the department has made. To track progress of DOD's Y2K Program (see the figure of DOD's major Y2K program components on this page), he uses a monthly Executive Y2K Steering Committee meeting. This meeting focuses senior leaders within the department on critical Y2K issues and the status in dealing with them. Since March, the Steering Committee has focused much of its attention on testing, business continuity and contingency planning, and consequence management.

By its very nature, DOD is a stakeholder in international Y2K preparations. To protect its international interests, DOD has three primary outreach focus areas: NATO, host nation support, and Russia. Two stated goals for NATO efforts exist: 1) ensure the continuity of the Stabilization Force and the Kosovo Peacekeeping Force operations, and

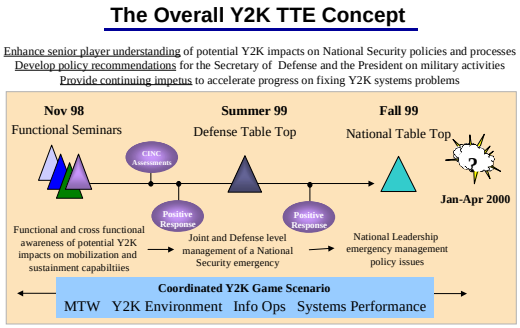
DoD Year 2000 Program
Major Components



2) obtain insight into the Y2K status of member nation systems that will affect other coalition operations. The potential Y2K impact on foreign-based U.S. military forces is far from defined. Finally, stability of nuclear arsenals and military-to-military Y2K cooperation are key elements of

DOD's Russian outreach.

To assess DOD's ability to respond with timely decisions in a Y2K degraded environment, the Chairman of the Joint Chiefs of Staff is conducting Exercise Positive Response Year 2000. This is a national level exercise conducted under scenarios of multiple Y2K failures. As a prelude to this exercise, the Department is conducting DOD level tabletop exercises that help prepare DOD leadership for potential Y2K national security impacts and for the national exercise. The overarching concept for the exercises is depicted in the figure.



Oversight of DOD Y2K activities and progress continues via several different organizations. Internally, the DOD Inspector General (IG) continues to perform audits and on September 3 issued its third summary report. This report summarizing 92 audit and inspection reports, briefings, and memorandums pertaining to DOD organizations, systems, and programs and their year 2000 conversion progress during the period from March through July 1999.

Externally, in addition to OMB reporting requirements for DOD, the GAO has an active audit program that has published a series of reports over the last couple years addressing the considerable Y2K related risks that DOD faces. It is currently focused on DOD's progress on completing and exercising business continuity planning as well as its management controls over the extensive high level testing or operational evaluations that are wrapping up.

Finally, the House and Senate have held hearings and issued letters, among other activities, to provide legislative branch oversight. Generally, the House has provided the detailed oversight of the executive branchs agencies' Y2K progress. However, during this session, this Committee has held three hearings one each during April, June, and July.

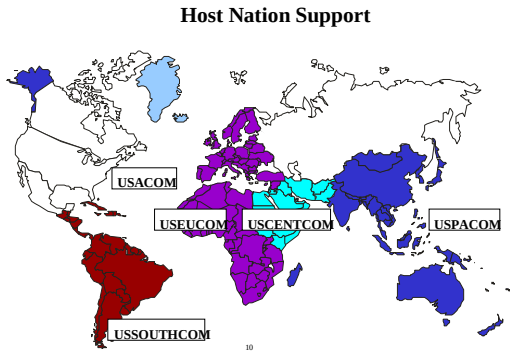
Status

The DOD is tracking 2,414 systems that it has identified as mission critical systems and another 7,229 non-mission critical systems for a total of 9,643. One hundred seventy seven, or 7% of its mission-critical systems, have not completed remediation efforts. It reports that 89% of mission-critical systems are compliant. The goal for all federal agencies to complete remediation of mission-critical systems passed on March 31, 1999. DOD forecasts that some of these remaining systems are not scheduled for completion until September while still others are not scheduled for completion until December 1999. These late scheduled completion dates leave little to no time for schedule slippage or unforeseen

events, which for IT-related projects are common. It underscores the need for realistic, tested contingency planning.

The DOD IG states that its audit results are consistent with DOD management progress reporting indicating that good progress is continuing to be made. Having said that, the audit results, which repeatedly reveal similar findings to those of GAO audits, also indicate that considerably more work is needed in several areas to ensure:

- adequate testing is performed;
- contingency plans are tested for viability;
- host nation support Y2K related risks to U.S. military forces and family members are adequately addressed;



- remaining noncompliant systems receive appropriate management attention; and
- military retiree pay and military hospitals, two OMB designated high-impact Federal programs, are compliant.

According to GAO, which published a series of reports on DOD's overall efforts to address the Y2K problem, DOD continues to face considerable risks. GAO is currently focused on assessing the progress in fixing non-compliant mission critical systems, the effectiveness of management controls, and high-level business continuity plans. It expects to issue a new report imminently reflecting findings and noting that the sheer volume, complexity, interconnectedness, and interdependency of DOD systems magnifies the possibility of Y2K related failures no matter how good its efforts are.

International outreach efforts have met with some success, however much work remains to address the many uncertainties and unknowns regarding host nation support issues. On September 13, the U.S. and the Russian Federation signed a joint statement indicating their intent to establish the Center for Year 2000 Strategic Stability (CY2KSS) during the Y2K transition period. The Committee Chairman and Vice-Chairman sent several letters encouraging the Russians to participate in the CY2KSS as well as other Y2K cooperative activities. Copies of the letters are contained in Appendix IV of this report. U.S. and Russian military personnel will sit side-by-side and continuously monitor U.S.-provided information on missile and space launches.

Although progress continues within NATO to address Y2K, it is unlikely that all will be well. NATO has raised the priority that Y2K receives by establishing a Y2K program office. However, the Committee is still concerned that the program office does not have the necessary authority and

clout to get the job done. Further, it is concerned that many NATO member countries have yet to make adequate progress addressing Y2K problems within key infrastructures such as power and telecommunications. Y2K failures in NATO systems and/or military systems and infrastructures of member nations could impact logistics support, force management, and US military facilities and personnel. The Committee has sent letters to the NATO Secretary General to outline these problem areas and suggest corrective action.

Concerns

- DOD remains behind schedule in completing its systems remediation and is at considerable risk of being unable to successfully meet the Year 2000 deadline.
- Regardless of how good a job DOD does in addressing Y2K, it has so many systems with an extreme number of system interfaces and interactions among external agencies and organizations, private sector organizations, and itself that the possibility of failure is increasingly magnified.
- Host nation support assessments may not be completed in sufficient time to adequately assess the risk to military forces and families and take adequate precautionary measures.
- NATO may not make enough progress to avoid Y2K failures. Ultimately, any Y2K related failures could result in reduced operational readiness and interoperability.

STATE AND LOCAL GOVERNMENT

This subsection reviews the readiness of governmental entities that are non-federal, including state agencies, county and city governments, and independent port authorities.[13]

Background and Vulnerabilities

As late as July 1999, as few as one in four counties, only two major U.S. cities, and only three states were reporting 100% Y2K readiness. While these alarming findings may reflect a lack of data and not a lack of readiness, contingency planning is obviously now paramount for governments and systems unable to make the transition.

As the Committee found in its February 1999 report, state and local governments deliver the majority of services and implement many federal programs upon which citizens rely. The massive scope of this sector, the critical nature of the services it provides, and the absence of uniform progress at all levels increases its Y2K vulnerability.

Taken collectively, the 87,000 local jurisdictions, 50 states, and 3,066 counties administer a larger information technology budget and more personnel than does the federal government.[14] State information systems, in connection with federal information systems, administer a

host of programs, including Medicaid payments, disability claims, and pollution monitoring.

What's more, local governments must provide the first response to crises, such as chemical spills, fires, the need for urgent care or human services, weather events, and civil unrest. In Y2K surveys, cities have identified their top four critical systems to be public safety, including management and jails; water and wastewater treatment; utilities; and finance. Adequate contingency planning is essential for dealing with potential Y2K failures. Such planning must involve all service providers in a local community, whether they come from local government or from local non-profit organizations.

Local governments must also plan for large public gatherings and the potential for increased criminal activity and/or civil unrest. Y2K poses a unique challenge to local officials, in that the ability of a municipality to respond to a situation may be compromised by the very breakdowns that precipitated the crisis.

[STATE AND LOCAL GOVERNMENTS]…"IS WHERE THE RUBBER HITS THE ROAD FOR FIRE AND POLICE, FOR PROGRAMS THAT… ALLOW COMMUNITIES TO FUNCTION AND THE ECONOMY TO GROW. IT IS VITAL THAT CITIZENS HAVE CONFIDENCE THAT COMMUNITY SERVICES WILL STILL FUNCTION AND THA THERE ARE REALISTIC CONTINGENCY PLANS SHOULD ANY SYSTEMS FAIL.
--- SENATOR DODD, JULY 15, 1999 HEARING

What Is Being Done?

Plans for the next few months involve substantial follow-up to previous surveys and existing initiatives.

The National League of Cities (NLC), the National Association of Counties (NACO), and the National Association of Senior Information Resource Executives (NASIRE) have all conducted additional rounds of surveys and extensive outreach activities. PTI, which manages the "Y2K and You" project for NACO and NLC, has contacted more than 18,000 officials about their Y2K preparations. Most recently, NACO and others have been distributing the publication, "Business Continuity Planning and Local Infrastructures: A Y2K Guide for Cities and Counties," written by the Center for Year 2000 and reflecting the new focus of Y2K preparation efforts. Despite this, the chair of the President's Y2K Council has frequently noted the inherent difficulty of penetrating county and local levels of government.

Private sector technology partnerships with nonprofit human service providers, such the nPower initiative in Seattle, seek to assist such organizations with Y2K assessments and remediation. Nationally, the Center for Y2K and Society, CompuMentor, and others have launched awareness campaigns, taken surveys, and provided Y2K workbooks. CompuMentor has sent out more than 14,000 workbooks to non-profits in the U.S. alone. The Center for Y2K and Society has recently surveyed a

number of cities in terms of general Y2K readiness, contingency planning, and community involvement.

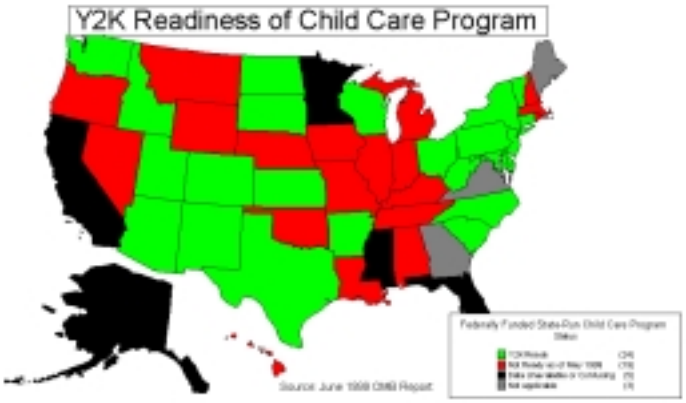
Some agencies or entities at the local and state level are planning short vacations in operations. For instance, as a precautionary measure, New York State court officials have ordered a one-week halt to scheduling new trials after January 1, 2000.

A number of county-wide or city-wide testing initiatives and contingency exercises have occurred in recent months and many more are planned. The city of Phoenix, Arizona, held a two-day Y2K-readiness test in July that involved outside telecommunications providers, the Red Cross, and multiple city departments. A number of table-top exercises are also taking place at the state and county level.

More sophisticated and realistic than table-top exercises are full-scale, multi-jurisdictional emergency operation simulations. The Washington, D.C., metropolitan area held such an exercise on September 1, 1999 with involvement from 35 organizations and more than 500 participants in 16 emergency operation centers. The exercise dealt with multiple failures across multiple sectors including transit, power, healthcare problems, public safety threats, pipeline ruptures, traffic jams, violence in prisons, chemical spills, and bad weather. Despite the pace of events, the jurisdictions and organizations involved were able to prioritize issues and take appropriate and collaborative action. The exercise illustrated the benefits of cooperation between providers and governmental agencies and across multiple and overlapping jurisdictions.

The President's Y2K Council has held regular telephone conferences with state Y2K managers and two summits since the beginning of 1999. These activities are expected to continue to assist with maintaining a high level of management focus.

Finally, the Committee held a state and local government hearing on July 15, 1999. Testimony reinforced the impression that there were widely different levels of preparedness.[15] Anecdotally, as in other arenas, major determinants of readiness were the size of the organization and financial conditions.



Status

States implement a host of federal programs, including programs for health and human services, agriculture, and the environment. The focus remains on 10 key state-

administered programs:

- Food stamps;
- Child support enforcement;
- Child nutrition;
- Low income housing energy assistance;
- Women, Infants, and Children;
- Childcare;
- Medicaid/MMIS and Medicaid IEVSn;
- Child welfare;
- Temporary Aid for Needy Families; and
- Unemployment insurance

A number of states did not plan to complete Year 2000 efforts until the last quarter of 1999, including eight states with respect to child support enforcement; five states with respect to unemployment insurance; and four states with respect to child nutrition. To date, four states have not achieved Y2K compliance for Medicaid systems, up from 17 in June 1999. However, of those reporting compliance, a number have not completed end-to-end testing. All told, states reported to NASIRE that they had a total of more than 15,000 mission-critical systems.

It is clear that some states are better prepared than others. NASIRE reports that, as of August 3, 1999, only three states were claiming completion of the implementation phase for all mission-critical systems. The bulk of the states, 38, reported being between 75% and 99% complete with implementation, up from an average of 65% at the end of May 1999. All states reported being actively engaged in internal and external contingency planning, but 14 states reported that the deadline for completing the plan was October 1999 or later.

The map in the Figure below shows the reported percentage of systems ready as of June 1999. In our judgment, less than 90% ready is cause for concern (yellow), while less than 70% is cause for some alarm (red). A few states did not report on the percentage of systems compliant, but do claim to be nearly ready.

Addressing external sources of vulnerability is a constant theme for Y2K, and is especially important for state and local governments. For instance, state officials in Pennsylvania recognized the interconnectedness and interdependencies of jurisdictions and the economy and launched a campaign that now extends to the federal government, 12 other states, Canada, and thousands of private companies.

According to hearing testimony from the Executive Director of the Indiana State Emergency Management Agency, the critical targets for which contingency plans are being developed are:

1. communication centers
2. emergency services
3. food service
4. health and medical services
5. power facilities
6. public facilities
7. public works
8. transportation
9. water and sewage facilities
10. loss of air handling systems
11. communications
12. back-up power systems
13. interruption of security systems
14. loss of public confidence

Indiana's plans have been developed in conjunction with the Federal Emergency Management Agency

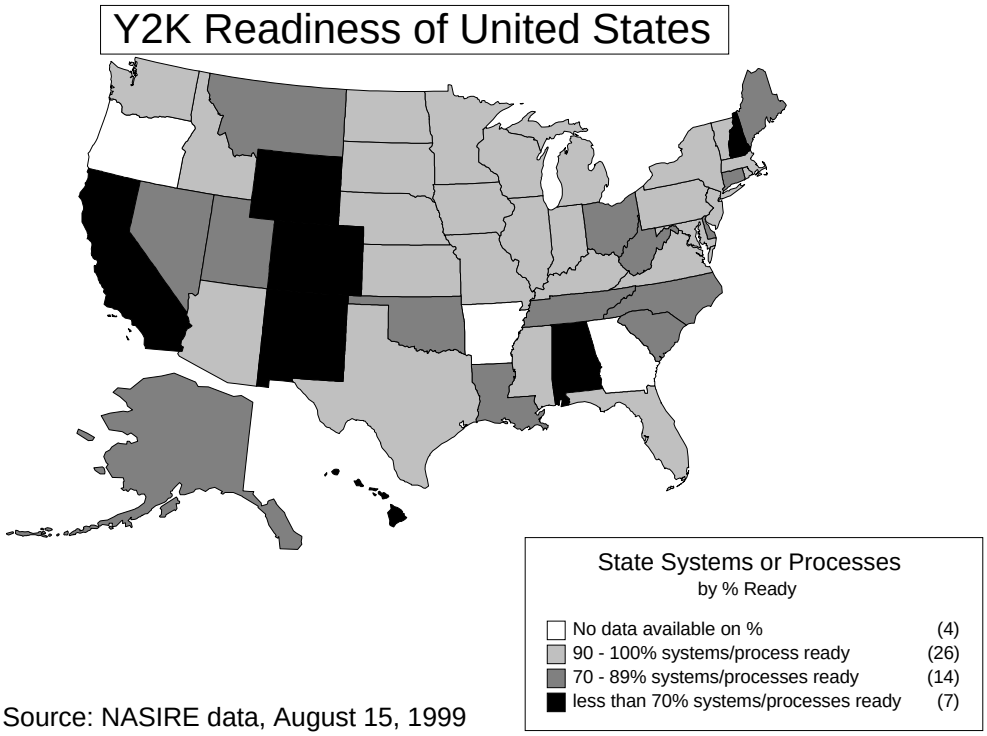
(FEMA) and enabled by an executive order of the governor. Such high-level management attention is a critical factor for successful implementation.

FEMA's role in supporting emergency management organizations is vital for coordination of multiple jurisdictions, particularly given the multitude of possible failures. FEMA has completed its first round of 10 regional meetings for state and local emergency management organizations and is in the process of follow-up meetings and table-top exercises.

results of their interviews are expected to be released soon.

As evidence of Y2K preparedness, there were no reported problems with the July 1, 1999, rollover date, which was relevant to the 46 states that began data-processing for fiscal year 2000 on that date. However, such evidence provides little predictive value since data issues for financial systems are only one small component of Y2K.

Recent surveys show that local governments, including cities and counties, are less well-prepared. According to a NACO survey, although only 27% of counties had completed system testing, contingency planning was still lagging: 74% of counties surveyed had or were developing contingency plans.



Source: NASIRE data, August 15, 1999

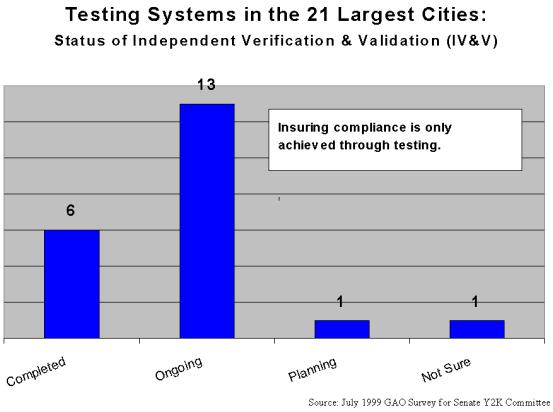
Florida has taken a very proactive approach to local government preparedness. Noting the lack of complete information about local governments, the State Year 2000 Task Force began a campaign to visit local jurisdictions with trained auditors from a variety of state agencies. The

Moreover, the NACO representative testifying at the Committee's July 15 hearing stated that some government entities may not have been entirely frank with their assessments or planning status, as they were finding it easier to report Y2K readiness than to deliver bad news. The California State Assembly, which has monitored state-wide progress notes the following about county preparedness:

"Counties...should not confuse the public by publishing that they are '98%' complete, when complete means that they are finished with internal remediation and testing. The interfaces that counties and the state maintain need to be addressed through end-to-end testing that has not occurred, consequently, these applications cannot responsibly deemed completed until the proper testing has occurred."[16]

NACO reports that spending by counties ranges from $10,000 to $100,000 for the smaller counties, to millions of dollars for the largest counties. At the high end of the spectrum is the County of Los Angeles, which has budgeted more than $155 million on its remediation program alone.

A GAO survey conducted in July 1999 of the 21 largest U.S. cities measured the readiness of key infrastructure components, as reported by city officials. At the time of the survey, only two cities were ready, and 10 cities reported that outstanding issues would not be resolved until the fourth quarter of 1999. As of mid-July, America's largest cities reported that, on average, they had completed 43% of the work that would be required for an uneventful transition to the Year 2000. While most of these cities plan to finish their tasks by September 30, a formidable amount of work remains unfinished, especially independent verification and validation.



On July 12, 1999, the NLC released a survey of 400 cities, which included the following results:

- 92% of respondents reported that all of their critical systems would be prepared by January 1, 2000;
- 92% said they have a citywide plan to address Y2K problems;
- 66% have prepared a Y2K contingency plan;
- Of those that have not developed a plan, 48% indicate they plan to develop one;
- 73% report they are working with public and private utilities;
- 59% are collaborating with other

municipal governments;

- 52% are working with business and private industry;
- 51% are working with county governments;
- 63% are using newspapers to disseminate information to the public about Y2K.

According to a January 1999 survey by the U.S. Conference of Mayors, about one-third of the 220 cities surveyed were planning to conduct citywide Y2K tests, and less than half had developed contingency plans. For the 136 cities able to estimate the total cost of compliance, such costs ranged from $2,000 to $59 million. Comparing these two surveys, one gets the impression that contingency planning is still not universal. Despite the optimism that all will be ready by December 1999, actual Y2K status is difficult to assess.

State and local governments also have primary responsibility for most elementary/secondary schools and post-secondary institutions. The status of their Y2K progress is disappointing.

In March 1999, the Department of Education and the National School Boards Association surveyed 16,366 school districts regarding their Y2K preparations. The survey period closed on May 28 with a 22% response rate. Only 42% of respondents had a written plan for achieving Y2K compliance. What's more, only 28% of respondents reported all their mission-critical systems then Y2K compliant; 72% said such systems were then or would be compliant by October 1; and 98% said their systems were then or would be fully compliant by January 1. If the respondents were a representative sample, the 2% of school districts reporting they will not be compliant by January 1 potentially represents about 1,820 schools, impacting about 340,000 students.

In May 1999, the Department surveyed 6,607 post-secondary institutions regarding their Y2K preparations. Only 61% had written plans for achieving Y2K compliance. Some 30% of respondents had mission-critical systems Y2K compliant; 60% said they would be ready by October 1; and 99% said they would be ready by January 1. These late readiness dates leave no room for error.

The Committee held a hearing on education and Y2K September 21.

Anecdotally, a number of stories paint a disturbing picture of widely different approaches and snafus.

- It was reported on June 14 that **California** had spent more than $400 million to test and repair computers to handle the date transition. However, as one sign of the confusion, officials could not tell whether the ultimate price for repair would approach $500 million or perhaps double that amount. In the most recent California status report, only 5 of the state's 116 departments were covered. The state's Y2K director recently stated it would take at

least one more month before his staff even identified all of the critical computer systems in the state—let alone fixed them.

- In **Bloomington, Indiana**, several people received checks for such amounts as $49 million and one cent, and $50 million. The checks had the correct amount in the numerical spot on the upper right hand of the checks--$49.01 and $50—but the words "forty-nine million" and "fifty million" on the center line. The mistake resulted from a computer error generated by new software that was installed to fix the Y2K problem. Local officials noted that it was ironic that these checks were coming from the check deception department.

- The South Florida Business Journal reported August 30, 1999, that according to Team Florida 2000, the State's official Y2K task force, **Miami Beach**, the site of a planned millennium celebration, is not ready for Y2K. Scott McPherson of Team Florida 2000 states in a report that "red flag" items include less than 70% compliance by April 1, 1999; Y2K implementation schedules as late as the fourth quarter; and no contingency plan in place.

Financial oversight or auditing of local governments by the state auditors' offices differs by state but, when applicable, such auditing has been occurring for Y2K. Moreover, a major source of operating and capital funds for governmental entities is the bond market. The municipal bond market appears to be positioning itself for lowered transactional risk during the rollover by discouraging transactions (settlements and issuance) at that time. One result has been an increase in the amount of available paper (bonds) during July and August.

However, Y2K does not seem to be hampering the ability of governments to raise funds in the markets. There has been no discernable Y2K discounting, despite information found in Y2K disclosure statements. One city reported that it explored the option of locking in interest rates over year-end for its debt, rather than risk weekly variable rates during the Y2K rollover. According to borrowers and underwriters, almost no one was engaged in such mode-switching, which suggested that the market was not concerned with Y2K impacts.

Expectations

In the months left, local governments will continue to remediate, test, and verify Y2K compliance. Large cities and counties, which have spent thousands of man-hours and millions of dollars, will likely experience few severe Y2K problems. These governments will have the expertise and equipment to make fixes where necessary. Small towns and rural counties, with few automated systems, will continue to discount the possibility of Y2K disruptions.

The vulnerability of such smaller entities is related to their dependence on larger governmental entities, including utilities and federal- or state-run assistance programs. The

ability of larger entities to assist local governments will likely be stretched to the limit by widespread Y2K problems.

Medium-sized governments, with perhaps fewer resources and more automation, face the more difficult problem. Surveys suggest that they have responded more complacently than have large complex organizations, assuming that they can "fix on failure" the few systems that actually fail. The expectation for such entities nationwide is that they will experience some dramatic failures in the hours, days, and weeks following the rollover date.

In most cases, such failures will not cause large-scale disruptions and will likely be fixed expeditiously. Possible failures include the degradation of police and fire dispatch capability, the inability to quickly access budget or financial data or to issue paychecks, regional airport closures, traffic problems due to traffic signaling failures, local hospital problems, degradation of local telephone service, and billing system problems for locally administrated utilities. The main concern is that such failures occur simultaneously and stretch thin resources. The impact on local economies could be severe over a six-month period.

Concerns

- The Committee remains greatly concerned about the ability of local governments to solve Y2K problems and doubts that adequate contingency planning has occurred.
- The ability of state systems to interact with federal systems continues to be an area of high concern; complete testing on the entire matrix of possible state-federal data transfers is nearly impractical at this point.
- Of utmost concern from a public safety point of view is the mixture of Y2K-hype, large millennium celebrations, and potential malicious attacks. This report highlights the need for local authorities to be ready to handle any situation, from hazardous waste spills to the failure of emergency 911 systems. While contingency planning and business continuity plans have become the norm for most state and local governments, there are few standards and little confidence that sufficient testing and verification of specific Y2K plans has occurred. This is particularly worrisome since communities may not be able to call upon external resources for a period of time.
- The safety net that provides emergency support and services to needy families and individuals is made up of thousands of non-profits and church organizations, many of which may have Y2K problems. A Y2K glitch could prevent someone calling a crisis line from getting the help they urgently need, or organizations from being able to mobilize quickly during a crisis.[17]
- Since most citizens interact with the government at the state and local government level, it is

vital that, in the remaining months, a high degree of confidence be built around their ability to respond to whatever Y2K brings.

EMERGENCY PREPAREDNESS AND EMERGENCY SERVICES

This sector is unique in that it will be immediately affected if serious failures occur, no matter what their nature or location. The Committee continues to stress the potential ripple effect of Y2K failures on different sectors of the economy and government, heightening the criticality of the emergency preparedness and emergency services.

Background and Vulnerabilities

The emergency preparedness and emergency services sector faces the dual challenge of preparing itself to provide services in the face of internal and external Y2K failures while bolstering emergency response operations for literally every other sector. The Y2K transition period could also potentially involve a dramatic increase in demand for service from these organizations on several fronts.

"ARE THEY (DISPATCHERS) PREPARED TO ADAPT TO A MANUAL SYSTEM WITHOUT COMPROMISING THE SAFETY OF THE OFFICERS?"

- AN 911 EQUIPMENT VENDOR

Technical or managerial failures in other sectors are only one source of the potential increased demand for service. The largely overlooked human behavior factor, and the still undetermined social dynamic that will in some ways shape the Y2K transition, could have an impact on demands for emergency service response that equals the impact on demand for emergency services related to technological failures.

Another aspect of the Y2K transition that will stretch the resources of emergency services is special events planning. Even if Y2K-related problems impose no additional response requirements on these organizations, the advent of the New Millennium on January 1 will be marked by the largest array of New Year's Eve celebrations in history, across the entire globe. Large public celebrations will be held in many cities across the country. Such public events, by their very nature, present major challenges to emergency service agencies, particularly for the law enforcement community.

An informal survey conducted by Committee staff indicates that major public events are scheduled in New York City, Washington, D.C., Chicago, Boston, and St. Louis, to name just a few. In Washington, D.C., a twenty-four hour celebration is planned beginning at 7 AM on December 31, when the New Year first arrives in the South Pacific. This celebration is expected to attract approximately 500,000 attendees to the Mall area. The "First Night Boston" celebration will include 60 separate venues throughout the city. Attendance at that celebration is expected to be

approximately 3 million.

At the Committee's March 30, 1999 field hearing in Las Vegas, Nevada, the Deputy Chief of the Las Vegas Metropolitan Police testified that the Las Vegas Convention and Visitors Authority estimates that upward of 700,000 tourists will visit Las Vegas to celebrate the arrival of the Year 2000. This figure represents almost double the number of visitors for last year's New Year's Eve celebration.

Emergency Services

Emergency service agencies, such as police, fire, emergency medical services (EMS), and the emergency management agencies, work together to form a seamless safety net and source of relief in time of disaster. However, this report addresses the remaining concerns about the emergency services agencies or "first responders" separately from those of the emergency preparedness/emergency management community. While in some areas their concerns overlap, some aspects of the Y2K problem affect one sector or the other differently.

Emergency service agencies may be asked to provide a broad array of services in response to Y2K problems, none of which may require the longer-range relief efforts or disaster response coordination efforts of their locality's emergency management office. Conversely, events could be of sufficient magnitude that the longer-term coordination efforts of the emergency management office become paramount in helping to manage emergency service and disaster relief resources. Although it is highly unlikely that the U.S. will confront a disaster of such magnitude, it is only prudent that potential Y2K "worst case scenarios" be at least considered as these agencies create contingency plans for Y2K. This represents an elementary principle of good emergency management.

In the months leading up to hearings before the Committee, a number of important efforts were undertaken by the Federal Emergency Management Agency (FEMA) and by professional associations of police, fire, and emergency management agencies, especially in awareness-raising. Based on available data, some local jurisdictions have not taken the problem seriously enough or have failed to provide information to key stakeholders. The lack of validated data creates a sense of vulnerability.

FEMA, Emergency Alert, and Law Enforcement Systems

In its prior report, the Committee emphasized the important role FEMA plays in coordinating the national response to disasters. The primary mechanism for coordinating this response is the Federal Response Plan (FRP), which outlines the roles of key federal agencies in fulfilling each of the twelve emergency support functions as designated. FEMA's role with respect to Y2K and the FRP is discussed in detail below.

Although the Committee is greatly encouraged by the activities of the emergency preparedness and emergency services sector associations,

one major issue remains of great concern: the Y2K-related vulnerability of the nation's Public Safety Answering Points (PSAPs). These are the emergency 911 call centers within which calls for police, fire, and emergency medical service assistance are processed. PSAPs function within a myriad of local jurisdictions across the nation, some within the framework of state-administered 911 regulatory commissions, and some outside any state regulatory framework. Complicating the task of assuring the readiness of these PSAPs is the fact that the Federal Communications Commission (FCC) has no regulatory authority over these centers, with the exception of radio frequency bandwidth issues. During the October 2, 1998 hearing on emergency preparedness, and in its February 1999 report, the Committee highlighted its concerns about the Y2K vulnerability of PSAPs. Although the preparedness of PSAPs is justifiably a major concern, the telecommunications industry has issued strong reassurances that basic emergency 911 services are expected to remain intact. In short, the proper steps have been taken within the telecommunications industry to assure that a citizen's call for assistance via the 911 system will be answered by the appropriate emergency service personnel. The remaining vulnerabilities regarding Computer Aided Dispatch (CAD) systems, an integral part of the overall 911 response system, are covered in detail in the following pages.

Also covered is the Emergency Alert System (EAS), which replaced the Emergency Broadcast System, and is the national emergency communications system through which government can rapidly disseminate information to the populace in times of local, regional, or national emergencies. The EAS is frequently used at the state and local level to warn of severe weather.

Lastly, law enforcement agencies at every level rely heavily on sophisticated information technology systems to do their jobs effectively and safely. Systems such as the National Crime Information Center (NCIC) and similar state criminal records and criminal justice information systems are a vital lifeline to all law enforcement officers. Without ready access to the important information these systems contain, a law enforcement officer's job becomes much more difficult, and potentially more dangerous. The Y2K vulnerability of criminal justice information systems and criminal records systems managed by local police departments and other criminal justice agencies remains a primary concern of the Committee.

What Is Being Done?

Recognizing the importance of the reliability of PSAPs, the U.S. Fire Administration (USFA) began a survey[18] of the Y2K readiness of PSAPs nationwide, beginning in December 1998. At that time, 19% of the 309 respondents were reporting full compliance. Additionally, 83% were in some stage of assessment, 72% were resolving problems, 53% had validated some or all of their solutions, and 45% had implemented

some or all of their fixes.

In a report released on April 14, 1999 by the Network Interoperability and Reliability Council (NRIC), the readiness of PSAPs was estimated to be only 10 percent. Updated information from the USFA survey provided to the Committee on April 23, 1999 indicated that, from a base of 770 responses received from 37 states, 87% stated they had plans for addressing Y2K problems and expected to be done before January 1. Disturbingly, only 40% indicated they had contingency plans to address potential Y2K failures.

On April 29, 1999, the Committee held a hearing on the impact of Y2K on 911 systems and local law enforcement. In his testimony before the Committee, FCC Commissioner Michael Powell provided an update on the Y2K readiness status of PSAPs, stating that 35% of the 5,456 PSAPs covered by service contracts from the nation's eight largest telephone companies were prepared for Y2K.

He noted that, by NRIC's estimates, there are a total of 6,739[19] PSAPs within the territories of the eight largest telephone companies. He emphasized that the higher number of PSAPs cited by NRIC represents only the best estimate of the phone companies, and the difficulty in determining the exact count of PSAPs only serves to point out the difficulties encountered in trying to address this issue.

Of particular concern was the low response rate to the USFA survey as of the date of the hearing (766 responses out of 4,300 surveys sent). The Committee asked the FCC and the USFA to work together to obtain readiness information from PSAPs that had not yet responded to the survey. At the request of the Committee, the USFA established partnerships with the Department of Justice and the FCC in an attempt to bolster the participation of the PSAPs in its assessment process. Using its network of local law enforcement and emergency service agencies, which receive federal grants, the Department of Justice contacted more than 5,000 agencies and asked them to help provide readiness information on 911 centers.

The USFA has reported that, in the first three days following the Department of Justice's efforts, 900 surveys were received. The USFA continues to work with the FCC by providing a list of PSAPs that have not responded. The FCC is working through its regulatory relationship with the telecommunications carriers to encourage the readiness of these PSAPs. NENA has also included a brief survey form requesting information on PSAP readiness on its web site.

Several cases have been reported in the media over the past year that highlight the problems faced by PSAPs. In 1998, Fairbanks, Alaska reportedly had to spend $100,000 on its 911 system, just 18 months after it was installed, in order to assure that it was Y2K ready.

In Pueblo, Colorado, city officials

learned in late June 1999 that it would be necessary to expend $160,000 for a new Y2K compliant 911 system, scheduled to be installed by September. The supervisor of another PSAP in the Washington, D.C. area told Committee staff that the desk-top PC based radio system in its dispatch center required a $60,000 patch. Without the patch, the department would have been unable to communicate with emergency units in the field at all. While such unexpected expenditures may not represent major budget items for large, well-funded cities, they could be the source of budgetary problems for smaller, less well-funded local governments. Contractor availability and installation scheduling problems have also been raised repeatedly as concerns by a number of emergency service managers.

The telecommunications industry has taken the necessary steps to assure that the portion of "enhanced 911" systems that provides a caller's address and phone number prior to the routing of the call into a PSAP will function properly. The equipment that is at risk is the CAD systems located within the PSAPs. The CAD systems consist of a series of locally owned or leased suites of computer equipment that fall outside the reach of local and long distance telephone companies, into the general category of what telephone companies commonly refer to as "customer premise equipment".

CAD systems enable 911 operators to efficiently and speedily handle calls for service, allowing them to provide the greatest amount of information possible to the responding units. CAD systems interface directly with a number of other information data bases within a PSAP, and they provide updated information on emergency service unit locations, directions to the location of a call, and records of previous calls for service received from a location or person. Such information is vital to an emergency service department in its effort to provide the safest, quickest, and most effective response to a call for help. For example, use of a CAD system enables a 911 operator to immediately provide a responding EMS unit with detailed information about a victim's prior medical problems. An operator also can provide police or fire department personnel about hazardous conditions encountered on previous occasions at a particular location to which they are responding through the assistance of a CAD system.

While a Y2K failure in a CAD system within a PSAP would not restrict a 911 operator's ability to dispatch an emergency service unit in response to a citizen's call for help, such failures would definitely lead to degradation of service within the PSAP. Without ready access to the information made accessible through the CAD system, the skill of the 911 operator becomes of prime importance. Much of the information usually provided by the CAD system must be obtained directly from the caller if the CAD system fails. Routing of the call within the PSAP to the proper emergency service division dispatcher (police, fire, EMS) must in most cases be done "manually"

through the utilization of an index card system in the event a CAD system fails.

Previously established response protocols for particular events or types of calls must be searched for by hand by the dispatcher and are not available as quickly as they would be via the CAD system. While none of these factors would prohibit a PSAP from functioning, they at the very least could complicate operations at a time when response requirements will potentially be higher than normal. The responsibility to remediate these systems falls squarely upon the police or fire department, or other local entity that operates them.

Emergency Preparedness

Planning for Y2K has consumed much of the attention of emergency management and disaster preparedness agencies at the federal, state, and local levels throughout the past year. Much of the contingency planning and crisis management efforts that have occurred at all levels of government for Y2K have been concentrated here.

Almost all of the agencies with which the Committee staff has had contact, plan to activate their Emergency Operations Centers (EOCs) as part of their jurisdictions' Y2K transition strategy. The crisis management structure that these organizations provide through the staffing of their EOCs will be a vital part of the overall Y2K disruption monitoring process and response nation wide.

The extensive contact the Committee has had with FEMA and state and local emergency management agencies indicates that much work has been done in the past year in preparation for the Y2K transition. Emergency management agencies at the state and local levels, working in conjunction with FEMA, have taken a strong leadership role in the area of Y2K emergency preparedness. FEMA, the National Emergency Management Association (NEMA), and the International Association of Emergency Managers (IAEM) have sponsored numerous initiatives focusing on Y2K emergency preparedness.

Awareness and State of Knowledge

Since January 1999, a variety of Y2K initiatives have been sponsored by the major professional law enforcement associations. Among these are the following:

- The January 1999 issue of the widely circulated FBI Law Enforcement Bulletin featured an article on the impact of Y2K on law enforcement information systems as its cover story.

- The March 1999 issue of Police Chief magazine, the official publication of the International Association of Chiefs of Police, featured Y2K as its cover story. The July issue discussed the importance of contingency planning.

- In March 1999, the International Association of Chiefs of Police initiated "Project Response: Preparing Law Enforcement for

Y2K", providing an excellent orientation to the Y2K problem for law enforcement and offering guidance on internal and community risk assessment, contingency planning, and incident command. It also includes a detailed Y2K resource directory.

- The Police Executive Research Forum, which serves large police agencies, disseminated a review of the Y2K preparedness checklists of its leading members.

- The National Sheriff's Association sponsored a Y2K workshop at it's Annual Conference in Columbus, Ohio in June 1999, where Committee staff provided a Y2K presentation.

- Numerous other Y2K initiatives and conferences have been sponsored by individual states, state-level professional associations, and regional groups in the emergency services sector throughout the past year.

During the April 29, 1999 hearing, the Committee heard testimony from the Department of Justice about its outreach efforts and the work of the Police/Public Safety/Law Enforcement/Criminal Justice Working Group of the President's Y2K Council. The testimony emphasized the importance of the ability of law enforcement to successfully engage in three activities: providing adequate police presence in the community, communications, and record keeping.

According to the Department of Juctice, in the area of emergency service communications, the good news is that many systems and devices will continue to operate satisfactorily, even in the absence of "Y2K certification". This viewpoint accurately reflects the technical assessments of the Y2K vulnerability of wireless radio communications within the communications industry that the Committee has reviewed. With the exception of the newer PC-based radio systems, little vulnerability is thought to exist in the area of radio communications.

The Department of Justice also pointed out the important role played by federal agencies, such as the Federal Highway Administration, EPA, Coast Guard, and Department of Interior.

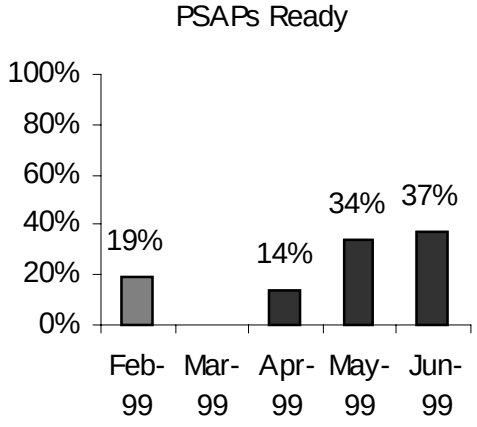
Status

The Committee wishes to reemphasize that while the readiness of the systems within a PSAP is of concern, this involves the issue of call processing efficiency, and does not impact the ability of a PSAP to receive its calls. The Committee has seen no indication that there will be any technical problems affecting a citizen's ability to pick up a telephone, reach a 911 operator, and ask for and receive emergency assistance. Our efforts in this regard are about assuring that these systems will be prepared to function in their totality, in the most effective and efficient way possible on January 1, 2000, in the same way they consistently function now.

At the request of the Committee, GAO completed an assessment of the Y2K vulnerability of the 911 system in spring 1999. In testimony before the Committee on April 29, 1999, GAO provided an easy to understand description of how 911 systems operate and where in the system Y2K vulnerabilities exists.[20]

In a report released on August 6, 1999, NRIC noted that Telco Forum data as of May 1, 1999 indicated that 34% of the PSAPs were prepared for Y2K, with 47% still with work in progress. No data was available for 19% of the PSAPs.

The Committee has focused much of its attention on the issue of PSAP readiness because it has the potential to equally impact the effectiveness of police, fire, and emergency medical service agencies. The most recent survey data on PSAP readiness, received by the Committee from the USFA on September 2, 1999 indicates that out of 2,200 responses received since January 1999, 92% have Y2K plans and expect to be ready before January 1.



As of June 30, 1999, 37% stated they were already prepared. However, only 55% indicated they had contingency plans in place.

Emergency Preparedness Network

Emergency management organizations at the federal, state, and local levels have been the focal points of much of the Y2K preparedness activities in the past year. Governments at all levels have recognized they will be relying heavily on these agencies as monitoring mechanisms, main coordination points for response to Y2K disruptions, centers for Y2K information collection and dissemination throughout the Y2K transition period. Equally important, these agencies serve as a reliable source of information on Y2K personal preparedness.

Like emergency services agencies, the emergency management organizations are faced with multiple challenges. They must prepare their own systems, be prepared to deal with internal and external systems failures effecting their own operations, and be prepared to respond to serious failures occurring in any other sector of their communities. Additionally, they must be prepared to simultaneously coordinate the relief effort in the event a natural disaster occurs in the time period surrounding the Y2K transition.

The Committee's February report outlined the potential role FEMA could play if Y2K disruptions were of significant magnitude to require that assistance be rendered by the federal government. In the past year, through the activities of its Catastrophic Disaster Recovery and Re-

lief Group, and its Preparedness, Training and Exercises Directorate, FEMA has served as an important resource to state and local government in the area of Y2K emergency preparedness.

FEMA's major activities since our last report have included the following[21]:

- Distributed 53,000 copies of "Contingency and Consequence Management Planning for Year 2000 Conversion – A Guide for State and Local Emergency Managers", and 83,000 copies of "Y2K and You: A New Horizon" personal preparedness guide.

- Conducted conversations with state emergency management agencies about development of a national consequence plan during regional Y2K workshops and tabletop exercises for the FRP.

- Continued efforts to obtain "early warning" information on Y2K consequences during the date transition period from counterpart emergency management agencies in other countries across 18 time zones east of the U.S., including involvement in formation of the Information Coordination Center (ICC), discussed later in this report. As of June, 24 countries had been contacted, resulting in 18 positive responses.

- Chaired monthly meetings of the President's Council's Domestic Interagency Working Group. This working group serves as a forum in which federal agencies can resolve high-level crosscutting policy issues related to Y2K.

- Jointly sponsored a survey of the state emergency management network with NEMA.

With regard to the NCIC, the Federal Bureau of Investigation (FBI), through its vast network of contacts with state and local law enforcement agencies, has waged an aggressive Y2K preparedness campaign in this area through the efforts of its Criminal Justice Information Services Division. The FBI provided testimony regarding its initiatives before the Committee at the hearing on local law enforcement and 911 systems on April 29, 1999.

The FBI's initiatives in this area began in 1996. The NCIC 2000 and Integrated Automated Fingerprint Identification System were scheduled to be Y2K ready and fully operational by July 1999. In the March 1999 quarterly report of the President's Y2K Council, NCIC was included on the list of key, high-impact federal programs**.** The September 13, 1999 OMB report indicates that all testing for the NCIC 2000 system has been completed. The FBI has made a standing offer of assistance to any state experiencing Y2K compliance difficulty.

In response to the Committee's concern about the lack of any formal assessment or general surveys addressing the issue of local law enforcement Y2K preparedness, the Attorney General, with the concurrence of the FBI Director, asked the

FBI's Criminal Justice Information Services Division to provide a status of national law enforcement and to assess each NCIC Control Terminal Agency (CTA). These agencies serve as the single direct connection to FBI for NCIC for each state. The assessment was conducted from May 24, 1999 through June 30, 1999. It evaluated three key areas: 1) NCIC - CTA connection readiness; 2) the broader Y2K preparedness of the state CTAs; and 3) Y2K awareness of local jurisdictions as it relates to their NCIC elements.

The Justice Department reported that all states, the District of Columbia, and Puerto Rico have successfully implemented connectivity to NCIC 2000. On broader Y2K issues, the CTAs of 44 states were fully prepared for Y2K. One state CTA was determined to be unprepared and was severely hampered by difficulties in procurement and staffing. Follow up for seven other CTAs that required additional attention is underway.

In the area of the Y2K awareness of local jurisdictions related to their NCIC elements, 12 states were fully prepared, 13 were found to have local agencies considered to be at high risk and unprepared, and 27 were found to have local agencies requiring some attention.

While we have viewed assessments of the readiness of the law enforcement community as reflective of the general preparedness of the emergency service community at large, there have been several noteworthy efforts to specifically assess the readiness of the fire departments and EMS agencies in areas beyond 911 communication.

- The USFA has been conducting a "show of hands" survey of mid- and upper-level local fire department officials during classes at the U.S. Fire Academy since April 1999. More than 1,600 students representing 750 departments and all 50 states have participated. 91% have indicated their departments are actively working to prepare for Y2K. 84% expect to be ready before the end of December, or are already compliant. 60% report having backup or contingency plans.

"I AM SOMEWHAT CONCERNED . . . THAT LAW ENFORCEMENT AGENCIES MAY BE CALLED UPON TO DEAL WITH Y2K-RELATED PROBLEMS THAT FALL OUTSIDE THEIR SPHERE OF . . . PREPARATION."

AN ASSISTANT ATTORNEY GENERAL

- The National Association of State Fire Marshals received approximately 500 responses in its survey of fire department readiness and found that 93% expect to be Y2K compliant by January 1.

- The USFA conducted a "snapshot survey" of 340 fire departments, representing 42 states. 85% of respondents stated that they were ready for Y2K now. An additional 12% stated that they will be ready before January 1. Three percent indicated that they would not be ready, and have no contingency

plans.

- The Emergency Services Working Group of the President's Y2K Council has had the responsibility of outreach to the EMS organizations. The Council's third quarter assessment noted that as of June 18, 1999, 72% of the state EMS agencies were reported to be totally Y2K compliant to perform EMS functions. It should be noted that approximately 65% of the EMS function in the emergency service sector falls within the jurisdiction of the fire departments.

"TERMINOLOGY SUCH AS . . . SPORADIC DISRUPTIONS HAVE CREATED A COMFORT FACTOR FOR SKEPTICS . . . COULD YOUR HOMETOWN BE SPORADICVILLE?"

CHIEF OF POLICE, HUDSON, OHIO

In May and June 1999, NEMA, in cooperation with FEMA, surveyed the Y2K readiness of the state and territorial emergency management agencies. The results of this survey were initially reported in the third quarterly report of the President's Y2K Council. The complete results of the survey are available on the NEMA website at www.nemaweb.org.

One mission critical system vital to public safety that was the subject of the NEMA survey was the EAS. According to FCC regulation, all broadcast stations and cable systems must participate in EAS, and others may participate voluntarily. Cable system providers serving populations greater than 10,000 subscribers were required to have their new EAS equipment in place and operational by December 31, 1998. The FCC has noted that the vendors of cable EAS equipment have certified that EAS equipment is Y2K compliant. According to the FCC, in May 1999, four major vendors of EAS equipment demonstrated Y2K compliance of their EAS equipment through test simulations of Y2K–related emergency event activation. In regard to EAS readiness, 61% of the respondents to the NEMA survey stated that their systems were compliant at the state warning point at the time of survey[22].

Federal Response Plan

In its previous report, the Committee emphasized the important role FEMA plays in coordinating the national response to disasters. The primary mechanism for coordinating this response is the FRP, which outlines the roles of key federal agencies in fulfilling each of the twelve emergency support functions as designated. In response to Y2K, FEMA has developed a supplement to the FRP that defines specific policies, planning assumptions, and response operations designed to address the unique challenges posed by Y2K. The Supplement emphasizes that the federal response to any Y2K related computer failures will be conducted in accordance with existing coordination mechanisms and procedures used in responding to the consequences of everyday disasters and emergencies.

By law, that response is limited to those events that exceed state and

local government capabilities to protect life, public health and safety, and property, and is based upon provisions of the FRP, Regional Response Plans, and the authority of the Stafford Act. The Committee has closely monitored FEMA's activities and the role it has played over the past 14 months in the area of Y2K preparedness. We have found that FEMA has made an invaluable contribution in its efforts to assure that Y2K will not impact the ability of the emergency management community to provide relief should disaster strike on January 1.

FEMA has been faced with the dual challenge of assuring the viability of the FRP, and ensuring that the Plan sufficiently addresses the unique problems posed by Y2K in the area of emergency preparedness. Many of FEMA's activities over the past year have focused specifically on those two goals. The Committee has reviewed the Y2K Supplement to the FRP and found that it provides a strong framework for monitoring Y2K events and coordinating the federal response to Y2K related emergencies in the event a state requests federal assistance.

Role of the National Guard

The first Committee report emphasized that the response to Y2K emergencies from the federal perspective will proceed in the same manner as it does for any other emergency. This also holds true for use of National Guard resources in the event of a Y2K-related emergency. State National Guard units will respond to requests for support from the governors of their respective states as they would in any disaster. If additional resources are needed, additional National Guard units could be requested from other states through their participation in Emergency Management Assistance Compacts (EMACs).

A clear history of mutual support exists in cases where an affected state's National Guard resources have been exhausted or were insufficient to address a particular disaster or other event. For example, in response to Hurricane Andrew, Florida National Guard units were supplemented with units from North Carolina, and, during the 1996 Olympics in Atlanta, Guard units from 47 states and territories were utilized.

Despite recurring rumors to the contrary spread on the Internet, the Committee can report in no uncertain terms that there are no plans for a "massive call-up" or "nationwide mobilization" of the National Guard in response to Y2K. In fact, the National Guard Bureau has advised us that the majority of the states (36 in total) currently have no intent to have any Guard units on standby or on State Active Duty in response to Y2K.

Sixteen states have indicated they will have individual soldiers or units on standby or on State Active Duty. Every state will man its National Guard Operations Center throughout the date transition. Fifty-one of the fifty four states, territories and the District of Columbia have completed and tested a formal Y2K annex to

their State Emergency Response Plans. These annexes address responses to multiple disasters, a loss of telecommunications for more than two hours, and a two-hour call up for units, if needed, on December 31.

The remaining three states and/or territories are in the process of completing and testing their Y2K annexes. The National Guard tested its High Frequency (HF) radio communications network in May 1999. During the exercise, 52 of 54 states and territories were successfully contacted. This would be a vital network in the event of major Y2K telecommunications failures.

Expectations

The emergency services and emergency preparedness sectors will likely be effected by Y2K disruptions that are of even modest proportion in many other sectors. With regard to emergency services—the "first responders"–our police, fire, and EMS officials are the people we often turn to for assistance, not only in times of grave danger, but also in times of utter confusion. The Y2K transition and arrival of the new millennium are likely to intersect in a manner that leads to a greatly increased demand for response from our emergency services. This may be due to technical failures in essential services, the need for additional support at major public celebrations, or any combination of unknowns that could result from the strange social dynamic that could potentially be created by public reaction to Y2K.

The Y2K awareness, preparedness, and contingency planning activities of the emergency services sector have increased significantly in the past year. The major emergency services professional associations have taken a much more active role in providing resources to their membership and in sponsoring Y2K initiatives since our last report. The Justice Department has successfully used the vast network of contacts the FBI maintains with state and local law enforcement to spread awareness, conduct assessments and identify problems. The USFA, the FCC, and the Justice Department continue to work together to spur much needed action on PSAP readiness. Many public safety officials have taken strong leadership roles in their communities on the Y2K issue. Despite all of these positive developments, this sector will face serious challenges due to Y2K, if for no other reason than the very nature of its responsibilities.

From the emergency preparedness perspective, emergency management agencies at the federal, state and local level will be major participants in monitoring and response mechanisms during the Y2K transition period. Governments at every level have relied heavily on their emergency management agencies to provide the framework for the planned response to potential Y2K disruptions. While the underlying causes of Y2K disruptions in vital areas such as utilities, transportation, and other public services may differ from those of natural disasters, the consequences of the failures in these areas and their impact on

the public are likely to be identical. The vast experience of emergency managers in responding to disruptions of vital services makes them uniquely qualified to manage the response to potential Y2K disruptions.

FEMA will continue to play a major role in planning for Y2K consequence management throughout the remainder of the year. It will serve as one of the major sources of input for the ICC, receiving data about significant Y2K disruptions from the national network of state and local emergency management agencies in the event any major problems occur.

Concerns

- The Committee has continuing concerns about the readiness status of the nation's PSAPs. It is not expected that failures in this area will prevent an individual from reaching a 911 operator, but an operator's ability to process a call in the most efficient manner may be affected. This could occur at a time when demands for emergency service are much higher than usual. There is no disagreement about the fact that failures in the CAD systems supporting our PSAPs would lead to degradation in service. The absence of any overall regulatory authority for these PSAPs makes assuring readiness in this area very difficult. The Committee's concern about the overall readiness of the emergency service sector is only one aspect of what has remained our broader concern about the readiness of local government nationwide. The impact of increased demand for services due to Y2K is also a major concern.

- Numerous articles and commentaries have been published throughout the past year that address the potential social dimension of both Y2K and "apocalyptic millennialism". This social dimension includes concerns about Y2K-induced public panic, consumer-induced shortages of cash and essential goods, Y2K based scams and other financial crime, survivalist-oriented behavior, fears of martial law, Y2K related conspiracy theories, mass suicides, increased opportunity for traditional types of terrorism and cyber-terrorism, and fears about the apocalypse.

- While the darkest of these Y2K fears are probably shared by only the very isolated few, the extent to which actual emergency service response might become necessary as a result of activities or events arising out of any aspect of this negative social dimension remains unknown. In the past year, news articles have reported a variety of strange events and behavior related to Y2K. In early 1999, police in Jerusalem interceded to disrupt a U.S.-based cult alleged to be planning violent activities at the arrival of the Millennium. Recently, Canadian officials, in cooperation with agents of the U.S. Bureau of Alcohol, Tobacco, and Firearms, arrested a man allegedly engaged in a plot to blow up part of the Alaska Pipeline on January 1 in fur-

therance of a scheme to defraud. The suspect allegedly planned to purchase oil futures, and increase his own profits by limiting the oil supply. Although we have no evidence indicating that such behavior or activities will increase or be widespread as we get closer to January 1, public safety officials may be confronted by similar problems, or by individuals motivated by sensationalistic or conspiracy-oriented rumors surrounding Y2K. These too must be considered as a potential impact of Y2K on the emergency services sector.

- Committee staff have discussed the Y2K issue with emergency service and emergency management officials from agencies across the country. While all agreed that Y2K presents significant challenges to them from both an internal preparedness perspective and added demand for service perspective, they emphasized that they did not expect Y2K to disrupt their ability to respond as needed.

THE INFORMATION COORDINATION CENTER

The global nature of the Y2K problem makes it imperative that the U.S. have a robust capability to monitor and respond to Y2K challenges that could adversely impact the nation. At present, there is no national coordinating mechanism linking all of the federal agencies' emergency operations. Further, there is no cohesive response structure integrating government and industry capabilities for the recovery of key information systems. In fact, the mere exchange of information between the private sector and the government is often fraught with problems.

Background

After the Committee's October 1998 hearing on emergency preparedness, the President's Y2K Council began discussing some type of command center that could enable the federal government to coordinate Y2K emergency response efforts at the national level. An amendment to Executive Order No. 13073, which created the Council, was in the works by December and was finally signed on June 14, 1999. In July, the Committee held a hearing to examine the role of the Information Coordination Center (ICC) in monitoring and facilitating Y2K response, recovery, and cyber-reconstitution.

According to testimony from John Koskinen, the National Security Council (NSC), the President's Y2K Council, and the Critical Infrastructure Assurance Office (CIAO) have developed the ICC to gather information about system operations in five areas: federal agencies; state, local and tribal governments; critical areas of the private sector; international; and cyber incidents.[23] The ICC will serve as the federal government's central point for coordinating a wide range of information on system operations and events related to the Y2K transition that will be collected by government emergency

operations centers and the private sector.

The ICC is intended to enable the government to monitor and track Y2K problems as they arise. The Administration hopes that, by providing a common picture of Y2K events, the ICC will be able to manage potentially adverse consequences. The amendment specifically authorizes the Chair of the President's Y2K Council to direct the ICC to help him:

- make preparations for information sharing and coordination within the federal government and key components of the public and private sectors;

- coordinate agency assessments of Y2K emergencies that could have an adverse affect on U.S. interests at home and abroad; and,

- if necessary, assist federal agencies and the Chair in reconstitution processes where appropriate.

The ICC will be supported by the General Services Administration (GSA). Its core missions will be carried out by officials from executive agencies (approximately 30-40 people) with expertise in important management and technical areas, computer hardware, software or security systems, reconstitution, and recovery. Agencies will also assign members of their public information staffs to participate in a Joint Public Information Center (JPIC), which will operate as part of the ICC. The JPIC will assist in providing information to the public and responding to inquiries, as well as helping agencies share information with their normal constituencies.

While the ICC strives to coordinate information, it must be more than a public relations center. In a crisis, it must also be able to respond appropriately by facilitating decisionmaking and coordinating response and recovery with a clear sense of national priorities.

The existing architecture within the government for collecting information in technology-related emergency situations includes about 15 emergency operations centers in agencies ranging from FEMA to the Department of State. All of these centers do an excellent job collecting information and receiving specific requests for federal assistance. No one of them, however, can collect and coordinate information flows about system operations from across the entire federal government; state, local and tribal governments; critical areas of the private sector; and countries around the world.

Sources of Information

Federal Agencies

The 24 Chief Financial Officer Act agencies will report to the ICC on systems operations status for the more than 40 high-impact programs that have been defined by the Office of Management and Budget. States, in particular, have asked for regular reports from the ICC on the status of

Global Positioning Systems, National Airspace Systems, the National Weather Service, the National Crime Information Center, the U.S. Postal Service, and navigable waterways.

State, Local, Tribal Governments

FEMA will give the ICC reports from state, local, and tribal governments. FEMA will expand its present system, which usually receives information on an exception basis where a request for federal assistance is made, to include regularly updated state reports on the status of such critical infrastructures as power, telecommunications, and health care. Since no capabilities exist for routine status reporting from local to state officials, the ICC will provide a software tool that local and state officials may use to facilitate this reporting and improve the depth of information provided to FEMA. If states do not currently have hardware or connectivity capacity to support such reporting activity, the ICC will provide a reliable and protected network-based service to receive and move the locally submitted information to the designated state facilities.

Private Sector

The President's Y2K Council has been encouraging critical industries to establish their own National Information Centers. These industry centers will collect status reports from individual companies and share this information with the appropriate federal emergency operations center (for example, electric power will provide information to the Department of Energy). Each federal agency will then analyze and summarize those reports and forward them to the ICC.

The electric power, oil and gas, telecommunications, and airline industries have already indicated they will have national information centers in place for the date rollover. Other sectors, such as water and health care, are more diffuse and will have greater difficulty formulating an adequate emergency reporting and response structure. The ICC is working with federal agencies and their associated industry organizations to encourage the formation of industry-led national information centers in these areas.

International

The Departments of State, Defense, and Transportation will give the ICC information about system operations outside the U.S. collected from our embassies, international organizations, and other posts. Numerous governments have indicated interest in exchanging data from the information centers they are creating, and Canada has requested an exchange of liaison officers to enhance coordination and status information.

The International Y2K Cooperation Center, established under the auspices of the UN and the World Bank, will use an ICC reporting format for international reporting purposes and will give the ICC additional international information about system operations abroad gathered from National Y2K coordinators.

Beginning at 7 a.m. eastern standard time on Friday, December 31,

when New Zealand moves into the Year 2000, much of the world will precede the U.S. into the next millennium. New Zealand, Australia, and the United Kingdom have expressed interest in providing early warning information on regional events as the date change takes effect in their respective time zones.

Cyber Incidents, Monitoring, and Response

The ICC is authorized by executive order to help facilitate "reconstitution" where appropriate. It is important that the government be able to articulate what it means by cyber-reconstitution prior to Y2K. The private sector and the government must learn to coordinate the recovery of key systems. At present, existing emergency response authorities for reconstitution of critical information systems are limited. If critical infrastructure systems were brought down by technological failures such as Y2K or an act of information warfare, the roles and responsibilities of government and industry are not clearly defined.

The Computer Emergency Response Teams (Domestic) and Forum of Incident Response and Security Teams (International) will provide reports to the ICC on any incidents within their respective areas. The National Infrastructure Protection Center (NIPC) at the Federal Bureau of Investigation, recently created to monitor cyber incidents; the CIAO; the GSA [GSA/Federal Computer Incident Response Capability (FedCIRC)]; the OSTP; the NIST; and the NSC will also provide information to the ICC and have personnel at the ICC. This arrangement will ensure that the NIPC will receive complete and timely data from all sources on unauthorized intrusions so it can conduct its missions of warning and response, in coordination with government and private sector entities.

The ICC will have direct connectivity for information sharing throughout the Department of Defense – Decision Support Activity (DSA) being formed specifically to monitor for Y2K. The DSA will coordinate the input for other key DOD agencies cooperating in this area, which include the Joint Task Force/Computer Network Defense; the National Communications Systems and its National Coordinating Center for Telecommunications; the Department of Defense Computer Emergency Response teams; the Defense Information Systems Agency and its Global Network Operations Security Center; and the National Security Agency. The ICC may also help coordinate assistance to agencies and sectors in cyber reconstitution processes necessitated by cyber incidents.

To succeed, the ICC must be realistic and pragmatic in the type of information it collects and coordinates. If it facilitates the reconstitution of critical cyber-systems, there must be some framework from which these new challenges are approached. There is clearly a pressing need to develop a national capability to rapidly bring vital government and private sector systems back online following a major disruption—no matter what the origin.

Using Information

The ICC is not a decision-making body. Information received by the ICC will be analyzed and a complete, regularly updated status report will be provided to agency decision-makers who will ultimately determine what, if any, federal actions are appropriate in response to Y2K-related difficulties. To help prepare for decisions that might have to be made, the Council has created two standing interagency working groups – one focused on domestic issues, and the other on international issues. These working groups meet regularly to review a wide range of issues and potential challenges that may confront agencies during the date rollover. As the end of the year approaches, the groups will meet as one to review overlapping challenges and resource demands for the agencies that may occur on January 1.

Although it will not provide reconstitution support to organizations that experience system failures, the ICC will be focused on how best to share information on the status of system operations to increase the likelihood that expert assistance is available to those who are in need and requesting help. The industry-led National Information Centers will have an especially important role to play in this area. In addition to giving the federal government and states reports on system operations in each industry, these centers will also be important resources for providing assistance to any organizations having Y2K-related difficulties.

Use of ICC Assets After The Year 2000 Conversion Period

The ICC is currently designed to sunset in March 2000 and will likely cost $40 to 50 million. The Committee continues to investigate what will happen to the expertise and capabilities developed in the ICC. The intellectual and physical capital created at the ICC facility will need to be managed by someone. It may be appropriate for the CIAO to be given the task of managing these assets and reporting the feasibility of integrating them into the initial operating capabilities of the National Plan. What will the government do with the lessons learned? What can the government learn from this process that might enhance long-term requirements for infrastructure protection?

The knowledge gained, capabilities developed, information channels established, and momentum created at the ICC will be an invaluable national asset--one bought and paid for by the American taxpayer. Like any valuable asset, we should take advantage of it and review ways to retain what is needed.[24]

The ICC experience during the Year 2000 conversion period will provide important contributions to the federal government's efforts to develop the plans and means for responding appropriately to significant cyber-events and emergencies. How, and in what ways, this capability is preserved after the Year 2000 conversion period must be given careful consideration.

Y2K is not a problem that will be neatly packaged and cleaned up by the time the world comes back to work on Monday, January 3. There is every indication that there will not be significant disruption in key U.S. systems. However, ensuring that the national security and emergency preparedness posture of the U.S. is not compromised is due diligence for the government.

Y2K is a watershed mark in the nation's understanding of critical infrastructures and their increasing dependency on information technology. As America's technological vulnerabilities increase, so does the need for a central mechanism to coordinate and reconstitute critical infrastructures and/or key information systems. The ICC could provide the first real world experience in dealing with these technological challenges of the information age.

Concerns

- Will lessons learned from Y2K help government and industry build a foundation for future collaboration on indications and warnings, as well as response and recovery mechanisms, needed to defend against information warfare or cyber threats?

- The ICC is trying to get the private sector to set up sector-wide information centers that would share information with the ICC. However, it is unclear what benefit the private sector would receive from sharing information. For example, would a company also receive "special" information from the government in return?

- How much could cyber-reconstitution cost the Government?

- What risks are created due to the lack of a common understanding of the definition of cyber-reconstitution?

[1] "Federal Government Year 2000 Preparedness: What's Next for Those Who Missed the March Deadline?", Apr. 14, 1999, S. 106-__.

[2] "Federal Y2K Spending: Where is the Money Going?", June 22, 1999, S. Hrg. 106-__.

[3] Director Jacob J. Lew, OMB.

[4] : "…with respect to information technology,…the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap years calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges data/time date with it." (National Institute for Standards and Technology)

[5] The guidance was developed by the GAO.

[6] Pub. Law No. 105-277 allocations only. Agencies have been using non-Y2K emergency funds to fix systems.

[7] Testimony of David Walker, Comptroller General of the U.S., to the U.S. Senate Special Committee on the Year 2000 Technology Problem and the U.S. Senate Appropriations Committee, "Federal Y2K Spending: Where is the Money Going?", June 22, 1999, S. Hrg. 106-__.

[8] "Federal Government Year 2000 Preparedness: What's Next for Those Who Missed the March Deadline?", Apr. 14, 1999, S. Hrg. 106-__.

[9] Ibid.

[10] Ibid.

[11] For obvious reasons, this information is not public.

[12] Ibid.

[13] Port authorities, which include airports, water ports, as well as special economic ports are often governed by specially elected or appointed boards, or fall under county management.

[14] Testimony of Randy Johnson, past president of the National Association of Counties (NACO), before the Committee on July 15, 1999.

[15] "State and Local Government Year 2000 Preparedness," July 15, 1999, S. Hrg. 106-__.

[16] "The Year 2000 Problem: Local Government and Critical Infrastructure Preparedness," July 1999, State of California Assembly Committee on Information Technology.

[17] Microsoft Corporation, "Y2K Day of Service," May 19, 1999.

[18] 4,300 surveys sent, preliminary results from the 309 received by USFA in February 1999.

[19] This number is much higher than the 4,500 PSAPs the Committee cited as being in existence in our first report. This earlier estimate was based on information provided by the Nine-One-One Emergency Number Association (NENA), and most likely did not include "secondary" or back-up PSAP facilities. Some PSAPs service multiple jurisdictions, complicating the task of obtaining an accurate count of how many actually exist.

[20] "911 and Y2K: Will the Call Be Answered?", Apr. 29, 1999, S. Hrg. 106-__.

[21] Many of these are available on the FEMA website. www.fema.gov

[22] An additional 15% percent stated that they would be compliant by January 1, 2000. Twenty percent did not respond, and 4% answered "not applicable" or "unknown". When questioned about EAS readiness beyond the state warning point, 46% stated they already were fully compliant, and an additional 16% stated they would be compliant by January 1. Thirty-one percent either did not respond, or answered "unknown". Seven percent answered "not applicable". It should be noted that there is no federal requirement for individual states or local networks to participate in EAS. The federal requirement for EAS is limited to providing a means for the President to address the entire nation simultaneously in time of national crisis.

[23] Testimony of John Koskinen, chairman, The President's Council on Year 2000 Conversion, July 29, 1999.

[24] Testimony of John Tritak, director, Critical Infrastructure Assurance Office, July 29, 1999.